PATRICK M. RYAN (SBN 203215)
pryan@bzbm.com
STEPHEN C. STEINBERG (SBN 230656)
ssteinberg@bzbm.com
GABRIELLA A. WILKINS (SBN 306173)
gwilkins@bzbm.com
BARTKO ZANKEL BUNZEL & MILLER
A Professional Law Corporation
One Embarcadero Center, Suite 800
San Francisco, California 94111
Telephone: (415) 956-1900
Facsimile: (415) 956-1152

Attorneys for Plaintiffs CISCO SYSTEMS, INC. and CISCO TECHNOLOGY, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CISCO SYSTEMS, INC. and CISCO TECHNOLOGY, INC. ,

Plaintiffs,

v.

SHENZHEN USOURCE TECHNOLOGY CO.; SHENZHEN WAREX TECHNOLOGIES CO., LTD.; and WAREX TECHNOLOGIES LIMITED;

Defendants.

Case No. 5:20-cv-04773-EJD

DECLARATION OF SECOND WITNESS IN SUPPORT OF PLAINTIFFS' EMERGENCY *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER, ASSET FREEZE ORDER, EXPEDITED DISCOVERY, ORDER PERMITTING ALTERNATIVE SERVICE OF PROCESS, AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

Date:
Time:
Courtroom: 4, 5th
Honorable Edward J. Davila

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

I, [redacted], hereby declare as follows:

1. I am familiar with the matters set forth in this declaration based upon my own personal knowledge. If called as a witness, I could and would competently testify to the following facts.

2. I submit this declaration in support of Plaintiffs' Emergency *Ex Parte* Motion for Temporary Restraining Order, Asset Freeze Order, Expedited Discovery, Order Permitting Alternative Service of Process, and Order to Show Cause Re: Preliminary Injunction.

3. I have determined that the purported Cisco® brand pluggable transceiver modules ("Cisco transceivers") advertised by and purchased from Defendants Shenzhen Usource Technology Co. ("Usource"), and Shenzhen Warex Technologies Co. and Warex Technologies Limited (together, "Warex") (collectively, "Defendants") by [redacted] are inauthentic, in that they were not manufactured by Cisco or by someone associated with Cisco, as these transceivers, including their sticker labels, housing and other components, and electrically erasable programmable read-only memory ("EEPROM"), exhibit characteristics that differ from genuine Cisco transceivers and also lack elements that are inherent to genuine Cisco transceivers.

Experience and Qualifications

4. I hold a Master of Information Systems and Bachelor of Science in Business Administration, both from University of Phoenix. I also attended California Polytechnic State University, San Luis Obispo, where I studied Electrical Engineering.

5. I began my professional career in 1985 as a product engineer for Hewlett Packard. During my fifteen years at Hewlett Packard, I became a manufacturing and product engineering manager. I was responsible for supervising product engineering teams, managing supplier product quality systems, customer audits and technical support, and conducting audits of product assembly. From 1999 through 2005, I worked at Agilent Technologies as a product engineering manager and R&D section manager, leading teams in new product development, intellectual property procurement, and post-release product quality. From 2005 to 2007, I worked as a product manager and product marketing engineer at Avago Technologies, where I managed certain transceiver module product market segments. From 2007 to 2008, I worked for TekXs Consulting

as a product authentication engineer, brand protection intelligence operation. At TekXs, I served as a consultant to Cisco Systems, Inc. ("Cisco"), coordinating, testing, and authenticating suspect counterfeit fiber optic transceiver products, and providing support to law enforcement authorities with authentication of Cisco products.

6. Since 2008, I have been employed by Cisco. During that time, I have served as a program manager and manager of operations in Cisco's Brand Protection Global Technical Intelligence Operations. As program manager, I was initially responsible for the testing, analysis, and authentication of Cisco products in the United States and Canada. I subsequently became responsible for monitoring, inspecting, and reviewing Cisco's products, including transceivers, on a worldwide basis. In this role, my team and I work to ensure that all products that we review are genuine—that is, manufactured by Cisco or one of its authorized manufacturing partners—and not counterfeit products offered by third parties seeking to capitalize on Cisco's brand reputation for building reliable, high-quality products. I am also responsible for investigating customer complaints, as well as non-conformances, or deviations, in product that can occur during the manufacturing process. I am therefore very familiar with Cisco transceivers and their component parts, and the manner in which they are labeled and packaged for domestic and international sale.

Manufacturing, Labeling, and Monitoring of Genuine Cisco Transceivers

7. A transceiver is an electronic device that uses fiber optic technology to transmit and receive data. A transceiver encodes and decodes data by converting an electrical signal into light pulses and then sends the data through a fiber optic cable, where it is received at the other end and converted back into an electrical signal. There are many models of Cisco transceivers which range in size, price, and functionality. Every Cisco transceiver, however, is designed to meet and exceed industry standards for quality, reliability, safety, and performance, which vary depending on the industry, e.g., there are higher standards for military-related applications than for standard commercial applications.

8. Cisco products are manufactured by, or often contain components that are manufactured by, third-party vendors called original equipment manufacturers ("OEMs"). Every OEM that Cisco utilizes is heavily vetted and scrutinized. The overwhelming majority of authentic

Cisco transceivers are manufactured by a number of OEMs, including [redacted]. These OEMs utilize specialized equipment and heavily-tested processes to produce a consistent, high-performing product on which consumers rely.

9. Cisco places strict control requirements on its OEMs, each of whom must adhere to high-quality manufacturing and distribution standards. These standards ensure that the product design meets feature specifications throughout the manufacturing lifecycle. Before a single product is shipped to a customer, Cisco conducts reliability demonstration testing to expose any undiscovered defects that may arise during the manufacturing process. After the product is approved for customer shipment, Cisco conducts ongoing reliability testing on subsequent productions. Cisco also ensures that each manufacturing facility meets its quality standards by subjecting each to stringent audits. Each OEM must maintain detailed production data records for each serialized product and must log product movement throughout the supply chain, which gives Cisco the ability to support customers via serial number traceability. Each OEM participates in quarterly business reviews that comprehensively examine the manufacturer's practices and procedures and identify areas for improvement.

10. Each authentic transceiver that is manufactured by an authorized OEM is assigned a unique top label that is controlled by Cisco, printed by a security company under contract with Cisco, and sent directly to the OEM. The top label incorporates a multitude of overt and covert security features. In addition to having the Cisco brand name embossed on the label, the top label bears a [redacted] then the product is a counterfeit.

11. Every Cisco transceiver also contains an EEPROM memory which stores a small amount of Cisco-specific data. The EEPROM content of an authentic Cisco transceiver [redacted]

[redacted] The absence of any of this data on an EEPROM is evidence that the product is inauthentic, as is the presence of any incorrect information. However, [redacted] then a Cisco host device will read it electronically as being a genuine Cisco transceiver.

12. Cisco maintains three lab facilities dedicated to testing potentially counterfeit products around the world, staffed by expert engineering investigators such as myself. The lab facilities are located in The Netherlands, Hong Kong, and San Jose, California—with this third facility being the largest. During the COVID-19 crisis, lab functions have been operating remotely at the homes of engineering investigators such as myself. Generally, products are analyzed by the expert engineer that is geographically closest to the procurement location. Access to products that are being tested is tightly controlled with only select members of the Cisco Brand Protection team being allowed to enter the labs or access the products being tested in order to ensure that a proper chain of custody is maintained and that there is no tampering with products before, during, or after examination.

13. Cisco's Brand Protection expert investigators are equipped with specialized tools to help them evaluate whether products are authentic.

Investigation of Counterfeit Products

14. As part of our investigation into the Cisco transceivers being offered online, [redacted] from Rowan TELS made purchases from Defendants.

15. For each purchase of a suspect Cisco transceiver from Defendants, the product was delivered to an address in [redacted]. Under a stringent chain of custody, each suspect product was then shipped to my home address at [redacted], where I have all of the equipment necessary to evaluate and analyze the products. I evaluated each product and determined (for the reasons set forth in the following paragraphs) that

every one of these products was in fact inauthentic, in that it was not manufactured by Cisco or by someone associated with Cisco. To confirm my analysis, I took photographs of the suspect transceivers and shared these photos with the OEM, if any, that was identified in the inauthentic top label. The OEM identified a set of potentially counterfeit attributes which were evaluated by the OEM's test engineer. Based on this evaluation, the OEM's test engineer also determined that the suspect transceiver was inauthentic. I reviewed the OEM's findings, confirmed those findings, and adopted them as part of my comprehensive analysis of each inauthentic transceiver.

Products from Defendant Usource

16. I understand that [redacted] purchased two transceivers from Usource, and that Usource advertised and offered these as Cisco-brand transceivers. Usource sent these suspect transceivers to [redacted] in [redacted]. [redacted] then sent the transceivers to my home address where I analyzed them.

17. Specifically, [redacted] purchased and sent me the following transceivers from Usource:

Product ID	Product Serial Number	Label Serial Number
Cisco SFP-10G-LR (Cisco Part Number = 10-2457-02)	FNS194307A4	WAMT755673
Cisco SFP-10G-LR (Cisco Part Number = 10-2457-02)	FNS194307A2	WAMT755673

18. On June 22, 2020, I examined both suspect transceivers received from Usource. Each suspect transceiver had a top label that bore the Cisco name and logo: cisco Each suspect transceiver had a top label that bore the Cisco Part Number SFP-10G-LR. Furthermore, the EEPROM for each transceiver identified the Cisco Part Number SFP-10G-LR, and included [redacted]. However, I determined that each transceiver sold by Usource is not a genuine Cisco product. I then prepared an Executive Summary Report ("ESR") detailing my findings.

19. I subsequently provided photographs of the suspect transceivers to [redacted], the OEM identified in the product serial number on the counterfeit top label. The photographs of each

product were reviewed and analyzed by the OEM's test engineer, who then prepared an ESR detailing his findings. [redacted] confirmed my assessment, determining that both suspect transceivers were inauthentic. I reviewed and adopted the OEM's findings as part of my final assessment.

20. The suspect transceivers sold by Usource are clearly inauthentic, in that they were not manufactured by Cisco or by someone associated with Cisco, due to the many differences between them and authentic Cisco transceivers. These differences include, but are not limited to:

[redacted]

Products from Defendant Warex

21. I understand that [redacted] purchased four transceivers from Warex, and that Warex advertised and offered these as Cisco-brand transceivers, including that they would read electronically as Cisco products when inserted into a Cisco switch. Warex sent these suspect transceivers to [redacted] in [redacted]. [redacted] then sent the transceivers to my home address where I analyzed them.

22. Specifically, [redacted] purchased the following transceivers from Warex:

Product ID	Label Serial Number
SFP-10G-LR-C	WX1150124421
SFP-10G-LR-C	WX1150124422
SFP-10G-SR-C	WX1150124431
SFP-10G-SR-C	WX1150124432

23. On June 22, 2020, I examined the four suspect transceivers received from Warex. Each suspect transceiver had a top label that bore the product IDs: "SFP-10G-LR-C" or "SFP-10G-SR-C." The SFP-10G-LR and SFP-10G-SR are two of Cisco's best-selling transceivers, but they do not normally include a "-C" at the end of each product ID. Furthermore, the EEPROM for each transceiver [redacted]. Because each transceiver included [redacted]," the end consumer would be deceived into believing these were genuine Cisco transceivers when they are not. A number of the [redacted]. The transceiver products under test contain a [redacted], not Warex. I determined that each transceiver sold by Warex is not a genuine Cisco product. I then prepared an ESR detailing my findings.

24. The suspect transceivers sold by Warex are clearly inauthentic, in that they were not manufactured by Cisco or by someone associated with Cisco, due to the many differences between them and authentic Cisco transceivers. These differences include, but are not limited to:

[redacted]

*****

25. In summary, all of the products listed above and purchased from Defendants share various distinctive characteristics that distinguish them from genuine products manufactured by or for Cisco. Those distinctive characteristics do not and could not appear on authentic Cisco transceivers. It is therefore my firm conclusion that all of the suspect transceivers sold by Defendants are inauthentic.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on July 14, 2020